REMARKS

Claims 1-21 are pending. Claim 7 has been amended. Claims 1-21 remain in the application. No new matter has been entered.

Claim 7 has been amended to correct a typographical error.

5   Claims 1, 5-9, 13-17, and 21 stand rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 6,088,804, issued to Hill et al., in view of U.S. Patent No. 5,960,170, issued to Chen et al. Applicant traverses the rejection.

To establish a *prima facie* case of obviousness: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge

10   generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there must be a reasonable expectation of success; and (3) the combined references must teach or suggest all the claim limitations. MPEP §2143.

A *prima facie* case of obviousness has not been established. The Hill

15   patent discloses a method of operating a dynamic network security system to respond to a plurality of attacks on a computer network having a multiplicity of computer nodes (Abstract). The system includes a plurality of security agents on associated computer nodes that are linked to a processor, which must first be trained to respond to attacks on the network (Col. 4, line 30 through Col. 5, line

20   6). In one embodiment, the security system is trained to respond to a plurality of training signatures that represent simulated network attacks (Col. 2, line 66 through Col. 3, line 3; Col. 6, lines 26-31; Col. 7, lines 9-17). A first attack signature is compared to each training signature to determine the training signature most closely resembling the first attack signature and the system is

25   adapted to respond by introducing the first attack signature as a new training signature (Col. 2, lines 4-16). In a second embodiment, security agents are configured to concurrently detect occurrences of security events characterizing a security attack and to process the security events to form attack signatures for display (Col. 3, lines 20-26). A trained processor is further configured to compare

30   the attack signature to training signatures to determine the simulated attack most

closely resembling the attack signature (Col. 3, lines 29-36). Finally, location identifiers identify the nodes in the network where security events may take place (Col. 6, lines 1-3).

5   Chen discloses an event-triggered, iterative computer virus detection system and method. Virus detection and treatment duties are divided between a client and server (Abstract). Computer viruses are iteratively detected at a client computer and a substantial portion of the tools and information required for the detection and treatment of the computer viruses is provided in a centralized location, such as a server (Col. 2, lines 62-67). The virus detection server

10   operates in conjunction with the client to determine whether viruses reside at the client (Col. 2, line 67 through Col. 3, line 2. A virus scan is initiated when a request is received or directed at the virus detection server and, once initiated, the virus detection server operates to iteratively detect and treat viruses associated with the client (Col. 2, lines 2-11). The virus detection server produces a virus

15   detection object, which is transmitted to the client and includes an executable program, and the virus detection object is specifically tailored according to previously determined conditions or conditions discovered as a result of the execution of previously produced virus detection objects (Col. 2, lines 13-20). The client executes the virus detection object and produces results that are

20   transmitted back to the virus detection server so that the server can produce additional virus detection objects based upon the results of the execution of the previous virus detection object to objects (Col. 2, lines 20-27). The iterative production and execution of virus detection objects is continued until a determination is made as to whether the targeted file or data on the client includes

25   a virus (Abstract).

First, the Hill and Chen patents, taken as a whole, do not provide a suggestion, motivation, or reason to combine. Hill and Chen are directed to solving different types of needs for respectively responding to network *attacks* versus detecting computer *viruses*. Specifically, a network attack attempts to

30   compromise a network by effecting the operation of one or more individual computer nodes. Thus, Hill teaches an approach to responding to network attacks

that first requires training the system to respond to a plurality of training signatures through the security agents (Col. 2, lines 66 through Col. 3, line 2; Col. 6, lines 26-31; Col. 7, lines 9-17). A processor detects a plurality of security events as detected by the security agents and occurring substantially concurrently

5   within a given sampling period sufficient to form an attack signature (Col. 1, lines 11-34; Col. 5, lines 29-38).

    In contrast, a computer virus primarily effects the operation of an single computer system. Thus, in one embodiment, Chen teaches detecting computer viruses in email messages. An initial virus detection object determines whether

10 any unread email messages reside at a client; additional virus detection objects can then determine whether the unread email messages include attachments, decode any found attachments and scan the decoded attachments to determine whether the unread messages include viruses (Col. 20, lines 9-18). A single virus detection object could be produced for each of the foregoing functions (Col. 20,

15 lines 18-24). However, at least one virus detection object must be produced by the virus detection server before being transmitted and executed by the client (Col. 20, lines 25-27). The results of the execution of the virus detection objects or objects are transmitted to the virus detection server so that the results can be analyzed (Col. 20, lines 27-29).

20   As a result, one of ordinary skill in the art at the time of applicant's invention would not be motivated or have a reason to combine the network attack response teachings of Hill with the computer virus detection teachings of Chen. Hill teaches security agents detecting security events on associated computer nodes that have occurred concurrently during a given sampling period, whereas

25 Chen teaches executing virus detection objects executing on clients and analyzing the results of the execution on a virus detection server. In other words, Hill teaches a wait-and-see approach whereby security events are passively detected while Chen teaches a trial-and-error approach whereby the virus detection server tries out combinations of suspect instructions that are executed by a client and that

30 can be used to determine whether a file includes a computer virus. Nor does Hill provide any suggestion to combine the teachings of *network attack* response with

the computer *virus detection* teachings of Chen.

In addition, Hill and Chen employ incompatible approaches to solving their respective needs. Hill teaches network attack detection and response by relying on a database of simulated attacks (Col. 5, lines 29-31). The processor

5   learns from accumulated training signatures to provide predictions of attacks that may occur on the network (Col. 5, lines 23-25; Col. 6, line 23 through Col. 7, line 46). In contrast, Chen teaches providing a substantial portion of the tools and information required for the detection and treatment of computer viruses and iteratively producing virus detection objects that are executed by a client (Col. 2,

10   line 63 through Col. 3, line 20). One of ordinary skill in the art at the time of applicant's invention would not be motivated or have a reason to combine the teachings of Hill with the teachings of Chen. Hill relies on learned attack signatures to determine the attack signatures to be compared and matched, whereas Chen relies on the detection of suspect instructions through iterative

15   execution of virus detection objects. Nor does Hill provide any suggestion to combine the teachings of network attack response with the iterative event-triggered computer virus detection taught by Chen.

Second, even when combined by picking and choosing selected parts, the Hill and Chen patents do not teach or suggest all claim limitations when

20   considered in light of the disclosure of each respective patent. Hill teaches processing security events to form attack signatures for use in *network attack* detection (Col. 5, lines 7-9 and 23-25). The security events may include port scans, malicious software, penetration attempts, and others that are included either through a specific code signature or through actions or attempts at actions (Col. 4,

25   lines 37-41). Thus, Hill fails to teach or suggest dynamically identifying each occurrence of a specific event sequence characteristic of behavior of a *computer virus* and the application which performed the specific event sequence, per Claims 1, 9 and 17.

Similarly, Chen teaches iterative computer virus detection involving

30   executing combinations of suspect instructions to determine whether a *file* includes a virus (Col. 19, lines 48-51). Simply, Chen statically analyzes files and

data and does not perform associative behavioral analysis of *runtime state*. Thus, Chen fails to teach or suggest tracking a sequence of execution of monitored events for one or more *applications executing* within a defined computing environment and dynamically identifying the *application* which performed a

5   specific event sequence, per Claims 1, 9 and 17.

Moreover, Hill and Chen teach away from dynamically detecting computer viruses through associative behavioral analysis of runtime state, per Claims 1, 9 and 17. Hill teaches detecting network events based on predictions of observed attack signatures formed from security events, whereas Claims 1, 9 and

10   17 define dynamically detecting computer viruses by analyzing behavior that can include both illegitimate actions performed by a computer virus and legitimate actions performed by the application. Likewise, Chen teaches computer virus detection involving analyzing targeted files or data to conditional determinations used in the detection of known and unknown computer viruses, whereas Claims 1,

15   9 and 17 recite tracking a sequence of execution of monitored events and identifying specific event sequences characteristic of computer virus and application behaviors. Thus, neither Hill nor Chen dynamically analyze computer virus and application behaviors.

Finally, if combined, the Hill and Chen patents do not provide a

20   reasonable expectation of success. When combined, Hill and Chen would produce an inoperative result. Hill teaches detecting network attacks by comparing an attack signature observed over a sampling period using a database of training signatures. Chen teaches providing computer virus detection and treatment through iterative execution of a plurality of the virus detection objects.

25   In combination, the teachings of Chen would provide computer virus detection on individual computer systems that could be combined with the teachings of Hill as security agents, but would fail to include the broader range of security event detection over a given sampling period also taught by Hill, as Chen fails to teach or suggest providing a sampling period in conjunction with the execution of the

30   virus detection objects. Moreover, such a combination would still be limited to providing network attack detection based on trained, retrospective knowledge,

and not dynamic associative behavior of runtime state, per Claims 1, 9 and 17. Furthermore, such a combination would fail to dynamically analyze computer virus and application behaviors since the security agents taught by Hill and the detection objects taught by Chen only identify where security events or suspect

5 instructions respectively originated and not what *application* caused such events or instructions, per Claims 1, 9 and 17.

Thus, a *prima facie* case of obviousness has not been shown with respect to Claims 1, 9 and 17. Claims 5-8 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited

10 therein. Claims 13-16 are dependent on Claim 9 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claim 21 is dependent on Claim 17 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown, withdrawal of the rejection of Claims 1,

15 5-9, 13-17, and 21 for obviousness under 35 U.S.C. 103(a) is requested.

Claims 2-4, 10-12, and 18-20 stand rejected under 35 U.S.C. 103(a) as being obvious over Hill et al., in view of Chen et al, and further in view of U.S. Patent 6,279,113, issued to Vaidya. Applicant traverses the rejection.

As argued above with respect to the rejection of Claims 1, 5-9, 13-17, and

20 21 for obviousness over Hill et al., in view of Chen et al., a *prima facie* case of obviousness has not been shown. Claims 2-4 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 10-12 are dependent on Claim 9 and are patentable for the above-stated reasons, and as further distinguished by the

25 limitations recited therein. Claims 18-20 are dependent on Claim 17 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown, withdrawal of the rejection of Claims 2-4, 10-12, and 18-20 for obviousness under 35 U.S.C. 103(a) is requested.

30 Claims 1-5, 10-13, and 17-21 stand provisionally rejected over Claims 1, 7-10, 11-20, and 21-28 of copending U.S. Patent Application, Serial No.

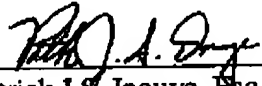09/580,375, filed on May 26, 2000. A Terminal Disclaimer is enclosed.
Withdrawal of the rejection for double-patenting is respectfully requested.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references

5 already applied.

Claims 1-21 are believed to be in condition for allowance. Entry of the foregoing amendments is requested and a Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

10

Respectfully submitted,

Dated: October 1, 2004

15

By: _____
Patrick J.S. Inouye, Esq.
Reg. No. 40,297

Law Offices of Patrick J.S. Inouye
810 Third Avenue, Suite 258
20 Seattle, WA 98104

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

OA2 Response